Dr Joe Purshouse (Senior Lecturer in Criminal Law and Justice at University of Sheffield); Dr Nessa Lynch (Associate Professor of Law at Victoria University of Wellington); Dr Marcin Betkier (Lecturer in Law at Victoria University of Wellington); Professor Liz Campbell (Professor and Francine V McNiff Chair in Criminal Jurisprudence at Monash University) — Written evidence (NTL0021)

1. Thank you for the opportunity to make a submission to the Justice and Home Affairs Committee's first inquiry: "New technologies and the application of the law".

2. We make this submission based on our research expertise. We have published numerous peer-reviewed academic articles on the regulation of new technologies, and have also co-authored a report on the regulation of facial recognition technology (FRT) in New Zealand, funded by the New Zealand Law Foundation.[1]

3. Here, we use FRT as a case study to highlight some of the structural weaknesses in the existing legal framework around new technologies used *in* the application of the law and draw attention to relevant examples of good practices from other jurisdictions for the Committee's consideration. We refer to the deployment of FRT by several police forces in England and Wales and the lessons that can be learned for the application of law to the regulation of other new technologies.

From our particular area of expertise, we formulate some principles which are of more general application.

Executive Summary

4. Whilst new technologies can bring considerable benefits to society, they shift the balance of power between the citizen and the state and can undermine fundamental human rights and democratic norms. The police trials of FRT were marred by inconsistencies and troubling practices, which were the product of a permissive culture around the deployment of high-risk technologies.

5. The police use of FRT in England and Wales has also exposed structural weaknesses in the legal framework governing the use of new technologies in a law enforcement context. Of principal concern is that the legal framework leaves

[1] This submission is draws upon, and develops, findings and insights from our prior work in this area, including: N Lynch, L Campbell, J Purshouse and M Betkier *Facial Recognition Technology in New Zealand: Towards a Legal and Ethical Framework* (November 2020); J. Purshouse and L. Campbell, 'Privacy, Crime Control and Police Use of Automated Facial Recognition Technology' [2019] Criminal Law Review 188; J. Purshouse and L. Campbell, 'Automated facial recognition and policing: A Bridge too far?' (2021) *Legal Studies* online first; N Lynch, L Campbell (eds.) The Collection and Retention of DNA from Suspects in New Zealand (VUP: 2015). Lynch is also currently (with Dr Andrew Chen) carrying out an independent review for New Zealand Police on the use of facial recognition technology in policing.

considerable discretion over the use of new technologies in the hands of law enforcement agencies which may tend to neglect the risks to human rights and to public trust which is, both, a prerequisite for, and an important goal of successful law enforcement.

6. The decision to use, or not use, a new technology should be guided by a robust legal framework, which requires external stakeholder consultation, transparency in the decision-making process, and independent oversight.

Police Use of Facial Recognition Technology in England And Wales And The Application Of Law

7. FRT is an algorithmic technology. It involves remote identification of an individual based on an analysis of the geometric features of the face, and a comparison between the features extracted from the captured image and one already stored. Several police forces in England and Wales have trialled the use of FRT in several contexts. These uses have included:

- using FRT software to verify the individual's identity by comparing a probe image against a database of images that the police control;
- using FRT to retrospectively identify suspects; and
- using live FRT. That typically involves the deployment of surveillance cameras to capture digital images of members of the public, which are then compared with digital images of persons on a pre-assembled 'watchlist' of images.

8. Whilst the use of FRT might bring considerable benefits in some circumstances, like with other advanced algorithmic tools, its increasing use has raised concerns regarding transparency, accuracy, and legality. The performance of FRT is not easily measured, as technological systems and algorithms vary depending on the task they are performing, and how 'success' is defined.[2] For example, an FRT system may be set at a particularly low accuracy threshold to maximise the number of identifications (with full awareness that this will also increase the number of false positive matches). The performance of FRT systems can also vary relative to the gender, ethnicity and age of individuals targeted, which raises concerns that FRT will manufacture, and reinforce any latent police discrimination against minority groups.[3]

9. Like fingerprint scanning and DNA profiling, FRT involves the processing of biometric information about the individual. However, FRT enables a data processor to collect biometric information remotely, so without individual cooperation or even awareness. Moreover, the automated technology allows the police to go much further in monitoring individuals as they occupy public space than ordinary/human observation would. The FRT process 'involves the creation of informational equivalents of body parts that exist outside their owner and are used and controlled by others.'[4] *R (Bridges) v Chief Constable of South Wales*

---

[2] P. Grother, M.M. Ngan and K. Hanaoka, Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification (NISTIR 8238, 2018).

[3] See J. Buolamwini and T. Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (Conference on Fairness, Accountability, and Transparency, New York, NY, 2018) 2; J. Buolamwini, 'Response: Racial and Gender bias in Amazon Rekognition — Commercial AI System for Analyzing Faces.' (Medium, 25 January 2019).

[4] P. Brey, 'Ethical Aspects of Facial Recognition Systems in Public Places' (2004) 2 J.I.C.E.S. 97,

Police,[5] confirmed that the police use of FRT to scan an individual as he traversed public space engaged his right to respect for private life under Article 8(1) of the European Convention on Human Rights (ECHR).

10. FRT may have a 'chilling effect' on public assemblies, freedom of expression, and the general use of public space by certain communities and demographics. Overt surveillance can damage legitimate political mobilisations in public space by undermining the perceived legitimacy of protest groups and limiting their access to resources.[6] Furthermore, the perception of being controlled in the public space breaks down the trust in police and other state institutions.[7] In the United Kingdom, football fans have responded to the use of live FRT at a number of matches by wearing face coverings or holding up signage to protest its use. When South Wales Police used live facial recognition at a football match between Cardiff City and Swansea City in January 2020, this prompted condemnation from football supporters' groups and civil liberties campaigners who argued that its use on football fans was unduly stigmatising.[8]

11. English and Welsh police forces have trialled or operationalised FRT since at least 2014, with South Wales Police,[9] the London Metropolitan Police,[10] and various quasi-private schemes[11] using it for policing and security purposes since this time. This is despite "the lack of a clear legislative framework for the technology".[12] Indeed, the Protection of Freedoms Act 2012 provides a legal framework for two types of biometrics, DNA and fingerprints, but does not apply to other biometrics such as facial images, gait, or voice. Instead,

12. In *R. (Bridges) v Chief Constable of South Wales Police and ors* [2020] EWCA Civ 1058, the Court of Appeal held that the respondent's use of FRT was unlawful as it was not 'in accordance with law' for the purposes of Article 8(2) of the European Convention on Human Rights (ECHR), and the South Wales Police had failed to carry out a proper Data Protection Impact Assessment (DPIA). The SWP also failed to comply with the public sector equality duty (PSED).

13. This was a significant judgment in which the Court of Appeal made clear that public authorities have a positive duty to take measures, such as independent verification, to ensure that the technologies they use for processing sensitive

---

107; see also K D. Haggerty and R.V. Ericson, 'The Surveillant Assemblage' (2000) 51 British Journal of Sociology 605.

[5] [2019] EWHC 2341 (Admin).

[6] V. Aston, 'State surveillance of protest and the rights to privacy and freedom of assembly: a comparison of judicial and protestor perspectives' (2017) 8 European Journal of Law and Technology 1, 10.

[7] Blake Schmidt "Hong Kong Police Already Have AI Tech That Can Recognise Faces" Bloomberg (23 October 2019)

[8] Football Supporters Europe "FSE Opposes Fans Being Used as Test Subjects for Facial Recognition Technology" www.fanseurope.org.

[9] https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf

[10] https://www.met.police.uk/live-facial-recognition-trial/

[11] Dan Sabbagh "Facial recognition technology scrapped at King's Cross site" The Guardian (2 September 2019).

[12] House of Commons Science and Technology Committee, The work of the Biometrics Commissioner and the Forensic Science Regulator, Nineteenth Report of Session 2017–19, 29; see also P. Fussey and D. Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (HRBDT, 2019).

personal data do not produce unacceptable demographic bias. However, in other ways, owing to the way the case was decided, the police may be able to make their FRT operations legally compliant through minor procedural amendments. For example, the Court of Appeal left open the possibility that an internal police policy document could be brought into accordance with the law for Article 8 purposes if it limited the discretion of individual officers as to who can go on a watchlist and where FRT can be used. The SWP could clear this low hurdle by making tweaks to its own internal policies, despite the absence of a positive legal basis for the police use of FRT beyond general common law powers.[13]

14. There are further areas of potential structural weakness in the legal framework regulating FRT and, by extension, other new technologies. Several guidance documents, such as from the Home Office Biometrics and Forensics Ethics Group (2018), and the Surveillance Camera Commissioner (2019),[14] seek to steer police practice in this area. Though these guidance documents may be cited in court, they do not provide actionable grounds for an individual to make a complaint. Moreover, non-compliance would not impact on the admissibility of any material gleaned. The Court of Appeal also found that the use of FRT by SWP was proportionate in the face of reasoned doubts about its operational utility and lingering concerns about the human rights implications of scanning hundreds of thousands of people to yield comparatively few arrests.[15]

15. It is telling that SWP is not appealing and in its own reaction, the Metropolitan Police Service gave clear indication that the judgment would not present significant obstacles to its own use of live FRT.[16] The United Kingdom has not introduced any specific laws relating to FRT. The framework regulating FRT is too generic and overlapping, in that it does not set out specific principles and rules for the use of FRT. We note that the trials of live facial recognition in England and Wales were marred by troubling police practices and inconsistent approaches between trialling forces, which suggest that the legal framework underpinning these trials was insufficiently narrow to adequately regulate the operations of FRT in a live public space surveillance context.[17]

Insights From Other Jurisdictions

---

[13] For further discussion of how the common law powers of the police have been extended beyond their appropriate limits, see Purshouse and Campbell (2021), n 1 above.

[14] Biometrics and Forensic Ethics Group Ethical Issues arising from the police use of live facial recognition technology (Facial Recognition Working Group, Interim Report, February 2019); and Surveillance Camera Commission The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems: Section 33 of Freedoms Act 2012 (March 2019).

[15] According to the MPS's own data, approximately 180,000 people were scanned across its 10 trials of FRT, leading to 27 people being engaged following an alert and just 9 arrests or other actions being taken based on an FRT match; Metropolitan Police Service and National Physical Laboratory *Metropolitan Police Service Live Facial Recognition Trials* (2020) p 3. For further discussion of the proportionality analysis of the Court of Appeal, see Purshouse and Campbell (2021), n 1 above; B. Keenan, 'Automated Facial Recognition and the Intensification of Police Surveillance' (2021) 84 *Modern Law Review* 886

[16] Metropolitan Police 'Live Facial Recognition' (Web Page), available at: https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/.

[17] See Purshouse and Campbell above n 1; P. Fussey and D. Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (HRBDT, 2019).

16. Whilst our analysis above has drawn attention to the links between a permissive legal framework and inconsistent approaches by the individual police forces to have trialled FRT, English and Welsh law has some strengths that other common law jurisdictions do not. In New Zealand, some human rights protections applicable to FRT surveillance are less entrenched in the domestic legal framework than in England and Wales.[18] For example, individuals cannot use domestic human rights legislation to advance a judicial review of the effect of a piece of legislation or policy affecting their rights. Moreover, New Zealand's Privacy Act 2020 does not offer the same level of protection for the collection and processing of FRT data as the European's Union General Data Processing Regulation (GDPR) or the UK Data Protection Act 2018. The Privacy Act 2020 does not distinguish stricter rules for technologies involving the processing of sensitive biometric data (like FRT), and does not require that the use of FRT must be 'strictly necessary and subject to appropriate safeguards for the rights and freedoms of the data subject'.[19] However, New Zealand Police are proceeding with more caution in this context, viewing organisational understanding of the legal and ethical implications of FRT as part of an end-to-end process involving multiple stakeholders, rather than rushing ahead with operational deployments that push the boundaries of discretionary legal frameworks.[20]

17. Despite sharing a broad alignment with England and Wales in terms of legal structure - particularly as far as the applicability of human rights and data protection provisions to the police use of FRT is concerned - the Scottish Government has emphasised the need for assessment of human rights impact prior to the introduction of any technology, not afterwards as occurred in England and Wales. While Police Scotland's 10-year strategy, *Policing 2026*, included a proposal to introduce FRT,[21] a Scottish parliamentary committee was highly critical of this plan. It concluded that there is no justifiable basis for Police Scotland to invest in this technology, and that prior to any decision to introduce it a robust and transparent assessment of its necessity and accuracy should be undertaken.[22] A subsequent response from Police Scotland indicated that it would ensure safeguards are in place prior to introducing FRT and agreed that the impact of its use should be fully understood before it is introduced.[23]

18. The experiences of New Zealand and Scotland show that in England and Wales pervasive FRT surveillance is the product of both structural legal weakness *and* cultural permissiveness of surveillance. We endorse the approach of the

---

[18] For further discussion of the regulation of FRT in New Zealand, see Lynch et al, above n 1.
[19] see Lynch et al, above n 1, p 74.
[20] see https://www.police.govt.nz/news/release/police-engages-experts-better-understand-facial-recognition-technology; Lynch et al, above n 1. M Mann and M Smith 'Automated facial recognition technology: recent developments and approaches to oversight' (2017) 40 University of New South Wales Law Journal 121.
[21] Police Scotland and Scottish Police Authority *Policing 2026: Our 10 year strategy for policing in Scotland* (2017), available at: https://www.scotland.police.uk/spa-media/jjkpn4et/policing-2026-strategy.pdf?view=Standard.
[22] Justice Sub-Committee on Policing, *Facial recognition: how policing in Scotland makes use of this technology* SP Paper 678 1st Report, 2020 (Session 5) 11 February 2020.
[23] Letter from Assistant Chief Constable Duncan Sloan to Justice Sub-Committee Convener, 8 April 2020, available at https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/20200410_PStoJF_Facial_Recognitio....pdf.

Scottish Government that has emphasised the need for assessment of human rights impact prior to the introduction of any technology, not afterwards as occurred in England and Wales. Moreover, the parliamentary report's foregrounding of communities and consent to policing is key.

19. The European Union is moving to regulate high-risk forms of artificial intelligence, particularly live biometric tracking (of which live automated FRT is an example). In April this year, a useful example of regulation which seeks to constrain high-risk uses of artificial intelligence has been promulgated in draft form by the European Union (EU). The Rules for the development, placement on the market and use of AI systems based on a proportionate risk approach (Draft AI Rules) strive to create a comprehensive list of technology-based risks and apply to them a coherent regulation framework depending on the level of risk.[24]

20. The EU is a major world market, and if the Draft AI Rules are adopted, it will have a significant effect and influence on tech development and commercial strategies even outside the EU. When enacted, those rules may set a global standard for the use of high-risk technology in a similar way as did the GDPR, the standard setter for data protection even outside the limits of the EU territorial jurisdiction, where compliance is not strictly required.

21. Some features of the Draft AI Rules are worth highlighting, as they pertain to the focus of this inquiry. Most pertinently for this inquiry, the Draft AI Rules set out in Article 5a list of 'prohibited AI practices', which include prohibition of particular uses of the AI systems by public authorities:

- the use of 'real-time' remote biometric identification systems (such as FRT) in publicly accessible spaces for the purpose of law enforcement, unless they are strictly necessary for the objectives listed in Rules, specifically evaluated against the potential consequences of not using them and against the list of risks to the rights and freedoms of the persons concerned. The use of those systems has to be subject to necessary and proportionate safeguards, and, importantly, subject to a prior authorisation granted by a judicial or an independent administrative authority;
- placing on the market, putting into service or use of the systems that evaluate or classify people based on their behaviour or personal characteristics (scoring systems).

22. Draft AI Rules also list in Annex III the areas in which the use of AI systems is deemed to pose high-risk. That includes the following technologies that may be used in the application of law:

- 'real-time' and 'post' remote biometric identification of natural persons;
- evaluation of the eligibility of natural persons for public assistance benefits and services;
- dispatching or establishing priority in the dispatching of emergency first response services (e.g. firefighters or medical aid);

[24] Proposal For A Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN.

- law enforcement uses, such as assessment of risk of offending, using polygraphs or assessing emotional state of persons, predicting the occurrence of a crime;
- use of technology for the purposes of migration, asylum and border control management; and
- assisting a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts.

The use of the high-risk AI systems listed above has to be subject to additional obligations and requirements specified in Title III of the Draft AI Rules.

23. It is likely that the Draft AI Rules will be changed to include the result of the ongoing extensive consultation process.[25] We believe that they should be further improved and their emphasis on protection of fundamental rights should be further strengthened.

24. Following our case study of the high-risk FRT systems, the Draft AI Rules regard 'remote biometric ID' which would include live automated FRT, as:[26]

> "particularly intrusive in the rights and freedoms of the concerned persons, to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights. In addition, the immediacy of the impact and the limited opportunities for further checks or corrections in relation to the use of such systems operating in 'real-time' carry heightened risks for the rights and freedoms of the persons that are concerned by law enforcement activities."

To mitigate the risks, the regulation would:

- Define 'public space' for the purposes of remote biometric ID systems as "any physical place that is accessible to the public, irrespective of whether the place in question is privately or publicly owned."
- Regard remote biometric ID in public spaces as 'particularly intrusive' and prohibit its use except where it is strictly necessary to achieve substantial public interest. Examples of permitted uses include threats to life, terrorism, search for victims of crime, and detecting serious crime (defined as attracting a term of imprisonment of three years or more).[27]
- require in advance specific independent authorisation for any use by law enforcement, except in cases of extreme urgency.

Key Lessons and Guiding Principles For The Use Of Technologies In The Application Of The Law

25. Here we distil some principles/considerations which are mainly focussed on the use of new technologies in the policing and law enforcement spheres.

26. We believe that the use of new technologies shifts the balance of power between the citizen and the state, and can undermine fundamental human rights

[25] See, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements_en
[26] Ibid, recital 18
[27] Draft Rules, recital 19

and democratic norms. Our recommendations go towards elimination or mitigation of many of these risks. This can be done by introducing necessary regulatory measures that should work in a systemic way to achieve that goal.

Assessing a spectrum of risk to individual and societal interests

27. Police and other law enforcement must, like rest of society, adapt to new technologies. Those technologies can have many beneficial and/or benign uses in policing, such as benefits in efficiency, convenience, freeing up time from unnecessary administrative tasks and improving the ability of police to detect and prosecute offending and to improve public safety. As an example – New Zealand Police's use of the OnDuty app which significantly reduces time spent on administration e.g. mapping crash sites. Police can record victim statements on their devices at family harm incidences and upload to a secure system meaning that victims do not need to give a separate statement later.[28]

28. However, the development of new technologies and deployment by law enforcement should not be considered an inherently valuable end-in-itself. Often the questions of whether a technology *should* be deployed at all are pre-empted or left solely to the discretion of individual police forces without a meaningful impact assessment.

29. Such impact assessments are necessary to manage risks that may be posed by adding new technologies or upgrading the existing ones. Adding new technologies may result in a multiplication of surveillance capability when the uses of technologies are combined or additional capacity is deployed. For example, if a Police force was to integrate FRT capability with body-worn video cameras, this could dramatically increase the scale and sophistication of the surveillance and so would require reappraisal of risks.[29] Similar effects of increased risk may be experienced when upgrading existing systems. In such cases, the increased impact may be made by technologies that speed up existing capabilities meaning more efficient processes (e.g. the use of analytical software on lawfully acquired CCTV footage) or the use of technologies that create new capabilities (e.g. emotion recognition as additional 'feature' of live FRT).

Consultation with communities

30. For all deployment of new technologies, but particularly where police operate without clear legislative framework or a high degree of discretion, community consultation with diverse communities is essential.

31. 'Policing by consent' is a foundational concept said to underpin the legitimacy of police in the United Kingdom. That means that public trust is the foundational element of effective policing. This is because policing is not possible *against* a democratic society. Also, creating and maintaining public trust should be one of the goals of policing.
32. There are concerns that the use of emergent technology without proper regulation may damage public trust and the legitimacy of Police, particularly if

[28] New Zealand Police 'Well and Truly on Duty' https://www.police.govt.nz/news/ten-one-magazine/well-and-truly-onduty
[29] K. Ringrose, 'Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns' (2019) 105 Virginia Law Review Online 57.

its use is not transparent or consensual. Police generally depend on the voluntary support and cooperation of the public to exercise their functions effectively, and this support is often contingent upon public perceptions of the manner in which police exercise their authority.[30] The Black Lives Matter protests that spread across the world following the killing of George Floyd in 2020 are a potent example of how excessive or discriminatory exercise of police power can rapidly lead to a breakdown in police/community relations.

33. If a technology is perceived to produce unfair or discriminatory outcomes or is used excessively in the absence of a prescribed legal framework, there is a risk that this will corrode the legitimacy of the police.[31] When subject to automated surveillance, it is important that the public can assess that any intrusion occasioned is lawful and justifiable

Clear purpose that is lawful and strictly necessary

34. For any deployment of emergent technology in policing, there must be clear purpose that is strictly necessary and lawful and other less intrusive methods and systems have been considered.

Accuracy rates

35. Accuracy rates must be established and meet a threshold of acceptability prior to use e.g. for facial recognition technology the system must return similar accuracy levels on ethnically diverse faces.

Human oversight

36. The degree of automation is an important consideration. Emergent technology that is fully or partly automated poses considerable risk to human rights. Human oversight should be required for any process that has significant potential impacts – e.g. facial recognition systems.

State access to private sector systems

37. Private sector surveillance systems (e.g. doorbell camera, neighbourhood camera footage aggregation) are rapidly increasing in use. It is important that oversight and other constraints which the state may impose on new technologies is not circumvented by access to unregulated and unaudited private sector systems. Any public-private collaboration in the use of new technologies should be demonstrably necessary and proportionate, with consideration given to the need for independent ethical oversight, vetting and high-level authorisation (such as by senior police officer, CPS or judiciary).[32]
Human rights, data protection and privacy impact assessments

---

[30] See, for example, Tom R Tyler "Enhancing Police Legitimacy" (2004) 593 Ann Am Acad Pol Soc Sci 84.
[31] B`. Bradford, J. Yesberg, J. Jackson, & P. Dawson 'Live facial recognition: Trust and legitimacy as predictors of public support for police use of new technology' (2020) *The British Journal of Criminology*, 60(6), 1502.
[32] See Biometrics and Forensics Ethics Group, 'Briefing note on the ethical issues arising from public– private collaboration in the use of live facial recognition technology' (January 2021).

38. Regulatory measures should either explicitly define the high-risk technologies or mandate the authorities that plan to use new technologies to carry out and publish the necessary risk analysis (for example, high-quality Privacy Impact Assessments, or Human Rights Impact Assessment). Then, the regulations should prescribe how to address the different levels of risks with the necessary measures improving accuracy, robustness, predictability, and transparency of the systems and, importantly, implementing oversight by an independent authority.

Transparency

39. Transparency will often be an important pre-requisite for ensuring that the use by law enforcement of new technologies is legally compliant and enjoys public confidence. Transparency is important not only insofar as enabling evaluation of particular technologies but also for ensuring that the decision-making process for the use of technology is open to public scrutiny. Examples of good practice include the publication of detailed impact assessments. For example New Zealand Police has recently commenced publishing a list of technologies in use in the organisation.[33]

Ongoing governance

40. A robust commissioning process is an important assurance but there are also risks in the operation of a technology for scope creep or inappropriate use after commissioning. It is important that oversight is not only tied to procurement, but is continual at each stage of the process of deploying a new technology.

Thank you for the opportunity to share our expertise for the benefit of the community. We would be pleased to provide further information on any of the points mentioned above.

3 September 2021

[33] New Zealand Police, Technology Capabilities List (July 2021) https://www.police.govt.nz/about-us/programmes-and-initiatives/police-use-emergent-technologies/technology-capabilities-list